



# STORE MANUAL

*Complete Operating Instructions for  
Store Managers and Employees*

**DO NOT REMOVE FROM PREMISES**



**Autobank XLViP Bill Validating Safes  
with CT8016 Control Panel Electronics**



a member of FireKing® Security Group  
101 Security Parkway • New Albany IN 47150  
Phone 800-452-4655 / 812-948-8400  
[www.fireking.com](http://www.fireking.com)

©2008 FireKing® Security Group  
Autobank with AuditLok® XLViP Electronics

*NKL,® Autobank,® and AuditLok® are trademarks of FireKing® Security Group.  
Other trademarks are property of their respective companies.*

# 1 HARDWARE FEATURES

## SAFE CHASSIS

Safes are equipped with one or two bill validators which secure funds behind one safe door. Your safe may be equipped with JCM, CashCode, or MEI brand bill validators. Validators may be bulk or single-note feed. Operational procedures are the same regardless of the specific validator hardware in your safe. Manual drops are securely stored in a separate locked compartment.

**Validator Compartment:** The validator door has a “T” handle. Internal sensors monitor door status to report unauthorized entry or if a door is left open too long. Doors have welded hinges and swing open up to 180°. Do not attempt to clean hinges. Commercial cleaning chemicals will cause the hinge lubricant to break down, making it difficult to open or close the door. On select models the validator heads may be removable for cleaning, repair or replacement without opening the safe door.

**Manual Drop Compartment:** The manual drop compartment door has a knob operated lock. An internal door position sensor is also installed to monitor the manual drop door. A slot is provided in the manual drop door. Drop envelopes pass through a serrated anti-fish baffle. The location of the manual drop compartment is at the top on bulk validator safes and on the bottom on standard validator safes.



CT8016 Control Panel (Top View)

## CONTROL PANEL

The keypad, display, and printer are located on the front and the power switch and electrical connections are located on the rear.

**LCD Display:** The control panel features an 80 character (4 rows, 20 columns) liquid crystal display (LCD).

**Select Buttons (Blue):** Three blue buttons immediately below the LCD area are used to select options appearing on the bottom line of the LCD.

**F1 & F2 Buttons (Orange):** The **F2** button is used together with the numeric keypad for bill validation and drop features. **F1** is reserved for future use.

**Number Pad (Black & White):** Enter a number or make a numeric selection as if you were dialing a phone. Number buttons may also be used to enter letters where appropriate. The “1” button is also used to enter special characters. The “pound” (#) button may be used to enter a 1 in the ten’s place in order to enter a two-digit menu item number, switch upper and lower case letters when entering data, or enter a decimal point. The “star” (\*) button is used to enter the star character.

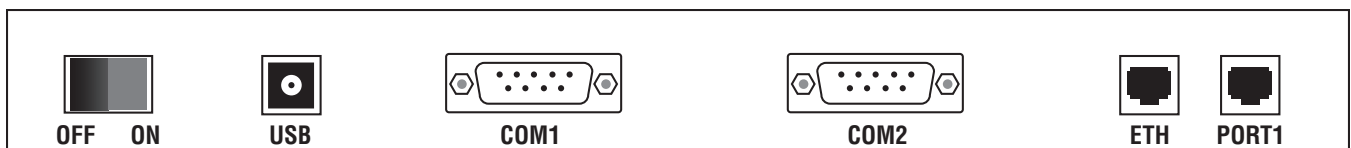
**Action Buttons (Orange with Icons):** To use any of these shortcut Action Buttons (located to the right of the number pad) log in, then press the desired Action Button:

- Door Access
- Manual Drop
- Validated Drop
- Print Report

**Scroll Buttons (Blue Arrows):** Use these arrow buttons to scroll up, down, left, or right. The right scroll button also activates and force-feeds the built-in printer.

**Printer:** A small thermal printer is built into the front of the control panel. Press down at the bottom of the printer cover and push toward the top to release the printer cover to replace standard 2 1/4 inch thermal paper.

**Power Switch:** The power switch turns on the control panel (the control panel is powered from the safe). The control panel should be switched off when connecting and disconnecting data from the safe.



Control Panel (Rear Connector Area)

**USB Connector:** Reserved for future use.

**COM1 & COM2 Connectors:** These RS232 serial ports are reserved for future use.

**ETH Connector:** The RJ45 “ETH” port is used to connect your safe to your local area network.

**PORT 1 Connector:** This RJ45 connector is used to connect the control panel to the safe. The control panel also receives its power through this cable, therefore the control panel will not function unless it is connected to the safe.

**Cell Phone SIM Card:** A small cover panel above the RJ45 ETH and PORT1 ports at the rear of the control panel protects the cellular phone SIM card. Remove the cover screw to access the SIM card slot. With the cover off, slide the SIM card holder to the “OPEN” position and gently pull it up to install or remove the SIM card. With the SIM card in place, press the SIM card flat against the circuit board and slide the SIM holder to the “LOCK” position to lock the SIM card in place. Replace the cover to protect the card.

**Cell Phone Antenna:** A cellular phone antenna is provided with your control panel. Connect the antenna to the threaded coax jack next to the SIM card cover (on some control panels this connector may be located next to the PORT 1 jack).



*Control Panel SIM Card Port  
(safe data and antenna cable  
connections also shown)*

## SAFE CONNECTIVITY (REAR PANEL)

Internal electronics store financial and security data and configuration settings. Bill validators, locks and sensors connect to the interior of the internal electronics assembly. Safe rear panel jacks connect external power, alarms, and control panel data to the internal electronics assembly. The backup side connections are reserved for service use only.

**Alarm Output Jack:** This RJ45 connector is used for connection to your facility alarm system. An alarm output interface cable is provided with the safe. The alarm output allows the safe to report burglary or duress conditions.

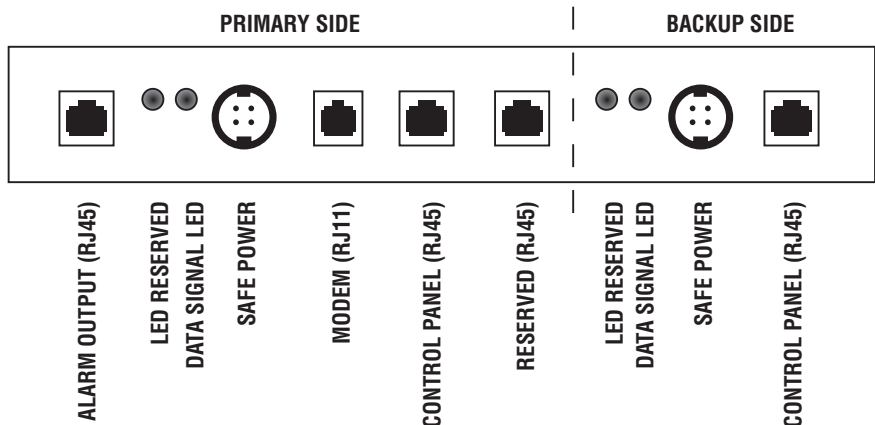
**Data Signal LED:** A small red LED will blink to indicate good data communication when the safe is powered, connected to the control panel properly, and the control panel is switched on and is fully booted up.

**Safe Power Jack:** One external power supply is used to provide the DC voltages used by the safe electronics. The power supply must be connected to the Primary Safe Power jack for normal operation. Plug the external power supply into a proper surge protector in accordance with installation instructions.

**Modem Jack:** Not Used.

**Control Panel Jack:** Connect the safe to the control panel using the RJ45/RJ45 cable provided.

**Backup Side:** The safe power and control panel cables should never be connected to the backup side except by authorized service personnel.



*Safe Rear Panel*

## GENERAL OPERATING PROCEDURES

### LOG IN

The following basic steps must be followed in order to log in and perform any cash handling operation. This same log in procedure is also used to access reports, remote supervision, general configuration settings, and other advanced software features.

1. Enter your Personal ID.
2. Scroll down to PIN: .
3. Enter your PIN.
4. Select login.
5. Select menu.

### CLOSE SESSION (LOG OUT)

In most cases leaving the screen untouched for about 30 to 45 seconds (typical) will result in the current session closing automatically. To close the active session immediately:

1. Back out to the main menu using the appropriate **Select Button** choices depending on your current menu.
2. Scroll down to Close Session.
3. Select select .

### DOOR ACCESS

Autobank XLV-iP validating safes have two compartments. One compartment is used strictly for validated drops. The second compartment is designed to be used for manual drops. The most common reason to open a safe door is to remove cash for bank deposit. Doors may have a delay.

1. Log in.
2. Choose Door Access, select select .
3. Choose the door to open, select enter .
4. If you are removing the money select YES (this will produce a deposit slip and zero the financial value of the compartment). If you are not removing the money, select NO.
5. If your profile does not bypass the door delay: Wait until the delay ends, then repeat Steps 1 to 4 again.
6. Turn the ACO key (validator compartment only), then turn the handle and open the safe door.
7. If you chose YES to removing cash a bank deposit slip will print automatically as soon as the door opens.
8. Complete your business inside the safe then close the door as soon as you are done. Failure to close the outer door in a timely manner will result in an audible alarm and a violation will be logged in the audit history.

### MANUAL DROP

The manual drop feature of your safe provides an alternative to the bill validators (generally for drops of non-cash such as checks, coupons, etc.). Use this procedure to document and count manual drops and credit the individual making the drop.

1. Log in.
2. Choose Manual Drop.
3. Select select .
4. Choose the desired manual drop location, select enter .
5. Choose the desired value type (coupons, checks, or cash), select enter .
6. Choose the desired currency, select enter .
7. Enter the amount, select enter .
8. If you are placing additional funds of any sort in the same drop select more, choose Add Item and select enter . If you need to edit the drop data select more, choose Edit Item, select enter , choose the item to edit. Repeat steps 5 to 8 as needed.
9. Optional: Your safe may be setup to ask for an envelop number and drop quantity. Enter the appropriate values and select enter at each screen.
10. The manual drop receipt will print. The screen will instruct you to add the receipt to your drop and make the drop. Select done to continue. A second receipt will print for your records.
11. Close your session.

### VALIDATE BILL

Use this procedure to authenticate a currency note without capturing the note in the safe.

1. Log In Method:
  - a. Log in.
  - b. Scroll as needed to choose Validate Bill.
  - c. Select select .
2. Bypass Login Method:
  - a. Press **F2**.
  - b. Press **0**.
3. Insert bill (screen will indicate Validation Mode).
5. The bill will automatically be rejected.
6. If the note is valid the screen will indicate Bill Verified and will indicate the currency and value. If the note is not valid an error message will appear.
7. You may insert additional bills as needed.
8. Close your session.

## VALIDATED DROP

This is the standard procedure to drop money in the safe using a bill validator. Using this procedure, every drop is credited to the individual making the drop and each drop event is unique.

1. Log in.
2. Choose Validated Drop.
3. Select select.
4. Choose the desired location and select enter.
5. Insert bills. A running total will appear on the screen as bills are validated.
6. You may switch to a bill count total rather than value total. If desired: select more, choose Quantity View, select enter.
7. Close your session.
8. A drop receipt will print automatically.

## EXTENDED DROP

Extended Drop is a feature that allows the validators to be continuously enabled to accept money without requiring users to log in each time.

### ACTIVATE EXTENDED DROP

1. Log in.
2. Choose Extended Drop.
3. Select select.
4. Choose the desired cash location
5. Select enter.
6. Choose the desired user.
7. Select enter.
8. Close your session.
9. The bill validator(s) will remain enabled and the safe will accept bills until Extended Drop is cleared.

### CLEARING EXTENDED DROP

Extended Drop is cleared automatically when the user's Operator report or the End Day report is run (Section 5). Extended Drop may be closed manually as follows:

1. Log in.
2. Choose Extended Drop.
3. Select select.
4. Choose the cash location.
5. Select enter.
6. If desired you may check the total for the current Extended Drop by choosing View Detail and selecting enter. You may then exit without clearing Extended Drop by selecting close.
7. Select YES to close the current Extended Drop.
8. Close your session.

**Note: All users are logged out of Extended Drop if the control panel is switched off or loses power.**

## INSTA DROP

The Insta Drop feature allows users to make quick validated drops by pressing the **F2** button and the number on the keypad assigned as the Insta Drop ID.

### ASSIGN USER TO INSTA DROP ID

1. Log in.
2. Choose Insta Drop.
3. Select select.
4. Choose an Available Insta Drop ID key (1 to 9)
5. Select enter.
6. Choose the desired cash location then select enter.
7. Choose the desired user then select enter.
8. Close your session.

### USING INSTA DROP

1. Press **F2**.
2. Press the number assigned as your Insta Drop ID.
3. Insert bills. A running total will appear on the screen as bills are validated.
4. Select enter to end the drop and exit.
5. A drop receipt will print automatically.

### CLEARING INSTA DROP ID

A user is cleared from the Insta Drop ID list automatically when their Operator report or the End Day report is run. A user may be cleared from Insta Drop manually as follows:

1. Log in.
2. Choose Insta Drop.
3. Select select.
4. Choose the Insta Drop ID of the user to be removed.
5. Select remove.
6. Select YES.
7. Close your session.

**Note: All users are logged out of Insta Drop if the control panel is switched off or loses power.**

## MANAGING USERS

### ABOUT USERS

Up to 1500 users may be enrolled, each assigned one of up to 45 unique permission lists (profiles), each independently granted or denied door access. **In order to successfully manage users follow these basic steps:**

1. Before enrolling users, create all necessary User Profiles. A User Profile is a permission level. Your safe supports as many as 45 unique User Profiles.
2. Add users. Up to 1500 users may be enrolled in your safe. Personal ID and PIN are assigned by the individual enrolling the user. The Personal ID may be any unique numeric value from 1 to 9 digits in length. A sequential User Number is also automatically assigned by the system.
3. Enable door access for users as needed. Each user is authorized for access to specific doors independent of their profile.

### CREATING USER PROFILES

A "profile" is a user-defined permission level. **Profiles should be established before enrolling users.**

1. Log in.
2. Choose `General Settings` then select `select`.
3. Choose `Security` then select `select`.
4. Choose `Profiles` then select `select`.
5. Choose `New` then select `new`.
6. Use the keypad to enter the text name of the new profile. Select `next`.
7. Select `check` to give (checked) or remove (unchecked) time delay bypass (`Time Delay Ovrerr`). *This is normally done only for the Armored Car profile.* Select `next`.
8. Choose a parent profile (`ADMIN` is the highest parent profile). Use the **LEFT** arrow to choose. Select `next`.
9. Scroll down to check desired optional permissions and select (place a check next to) each option desired. Select `save`.
10. Select `YES`.
11. Close your session.

### ADD USER

Before adding users you should have already configured profiles.

1. Log in.
2. Choose `General Settings` then select `select`.
3. Choose `Security` then select `select`.
4. Choose `Users` then select `select`.
5. Choose `Enroll User` then select `select`.
6. There is no option for `User Identifier`. Press **DOWN** to advance.

7. Use the keypad to enter the user's first name. Press **DOWN** to advance.
8. Use the keypad to enter the user's last name. Press **DOWN** to advance.
9. Use the keypad to enter the user's `Personal ID`. Note: each user must have a unique Personal ID. The Personal ID may be any value from one to nine digits in length. Press the **DOWN** to advance.
10. Use the keypad to enter the user's `PIN`. The PIN should be at least 4 digits long. Press **DOWN** to advance.
11. Repeat Step 10 to confirm the `PIN`.
12. Use the keypad to enter the user's `Duress PIN`. This PIN is used to activate the duress alarm output. Press **DOWN** to advance.
13. Repeat Step 12 to confirm the `PIN`.
14. Use the keypad to enter the `Bank account number` for deposits associated with this user. Press **DOWN** to advance. *Bank account numbers by individual is optional.*
15. Choose a `Profile` for the user (press **LEFT** to toggle through available profile options). Press **DOWN** to advance.
16. Choose the required `Login method` (press **LEFT** to toggle through available options). Press **DOWN** to advance.
17. Choose the `Language` to display for the user (press **LEFT** to toggle through available options). Press **DOWN** to advance.
18. Choose the desired `User Status` (press **LEFT** to toggle through available options; new users should be set to `ACTIVE`). Press **DOWN** to advance.
19. Select `save`.
20. Select `YES`.
21. Close your session.

### DOOR ACCESS BY USER

You may give or remove door access for each door by user as follows:

1. Log in.
2. Choose `General Settings` then select `select`.
3. Choose `Security` then select `select`.
4. Choose `Users` then select `select`.
5. Choose `Doors by User` then select `select`.
6. Choose the user to edit. Select `enter`.
7. To make a change select `update`.
8. Choose a door to add or remove from the user.
9. Select `check` to give (checked) or remove (unchecked) permission.
10. Select `save` then select "YES" to confirm.
11. Close your session.

## EDIT USER

Several user details may be changed including user PIN, duress PIN, bank account number, profile, login method, language, and status. Follow the steps of the Add User procedure except:

1. Log in.
2. Choose **General Settings** then select **select**.
3. Choose **Security** then select **select**.
4. Choose **Users** then select **select**.
5. Choose **Edit/View User** then select **select**.
6. Choose a user to edit then select **select**.
7. Press **DOWN** to advance through options. Select **update** at any time to begin editing options. Select **save** at any time to save changes and return to the user list. *For detailed information about specific options refer to Add User (above).*
8. Close your session.

## DELETE USER

Enrolled users may be deleted as follows:

1. Log in.
2. Choose **General Settings** then select **select**.
3. Choose **Security** then select **select**.
4. Choose **Users** then select **select**.
5. Choose **Delete User** then select **select**.
6. Choose a user to delete then select **select**.
7. Select **YES**.
8. Close your session.

## ACTIVATE (OR DEACTIVATE) USER

Use this procedure to activate a user who has been deactivated (or deactivate an active user):

1. Log in.
2. Choose **General Settings** then select **select**.
3. Choose **Security** then select **select**.
4. Choose **Users** then select **select**.
5. Choose **Activate User (or Deactivate User)** then select **select**.
6. Choose a user to activate or (deactivate).
7. Select **check** (checked state) to include the user.
8. Select **YES** to confirm then **OK** to continue.
9. Close your session.

## FORCE CHANGE EVERYONE'S PINS

You may force all users to change their PIN the next time they log in:

1. Log in.
2. Choose **General Settings** then select **select**.
3. Choose **Security** then select **select**.
4. Choose **Users** then select **select**.
5. Choose **Force Change PIN** then select **select**.
6. Select **YES** to confirm then **OK** to continue.
7. Close your session.

*Note: The next time you and all other users log in they will see a message that their PIN has expired. Refer to "PIN Expired Message" (below) for further instructions.*

## CHANGING YOUR OWN PIN

You may change your own PIN at any time as follows:

1. Log in.
2. Choose **General Settings** then select **select**.
3. Choose **Security** then select **select**.
4. Choose **Users** then select **select**.
5. Choose **Change PIN** then select **select**.
6. Enter your current PIN. Press **DOWN**.
7. Confirm your PIN. Press **DOWN**.
8. Enter a new duress PIN. Press **DOWN**.
9. Confirm the new duress PIN. Press **DOWN**.
10. Select **save**.
11. Select **YES** to confirm.
12. Close your session.

## "PIN EXPIRED" MESSAGE

If you have been enrolled in the system and you are logging in for the first time you will be required to change your PIN. If all user's PINs are forced to change you will also be required to change your PIN. In either case, respond to the PIN Expired message as follows:

1. Select **OK** when you receive the message that your PIN is expired and you must change your PIN.
2. Enter your current PIN. Press **DOWN**.
3. Enter your new PIN. Press **DOWN**.
4. Confirm your new PIN. Press **DOWN**.
5. Enter a new duress PIN. Press **DOWN**.
6. Confirm the new duress PIN. Press **DOWN**.
7. Select **save**.
8. Select **YES** to confirm.
9. Continue with whatever procedure you were originally logging in to perform.

# REPORTS

## ABOUT REPORTS

Nine unique reports may be requested plus four types of reports (including past drop receipts) may be reprinted. In most cases, summary style reports are preferred because they are short, concise, and include a complete summary. Detail version reports include the full summary version plus whatever additional details apply to the type of report selected. The Daily Close Report may be configured to print automatically at a predetermined time or may be printed manually. All other reports are initiated manually.

## PRINTING REPORTS

To print any report follow this basic procedure:

1. Log in.
2. Choose `Reports`.
3. Select `select`.
4. Choose type of report to print.
5. Select `enter`.
6. Several types of reports require you to answer a few additional questions in order to print the correct information. Follow the directions on screen to complete the report printing process.
7. The report chosen will print at the onboard printer.
8. Close your session.

## REPORT CONFIGURATION OPTIONS

Several report options may be configured as desired to meet the specific needs of your location.

### GENERAL REPORT OPTIONS

By default, receipts print automatically and you receive one copy of any report you print at the time you print it. You may edit these settings as follows:

1. Log in.
2. Choose `General Settings` then select `select`.
3. Choose `General` then select `select`.
4. Select `update` to enable editing of values.
5. Press **DOWN** to move through the list of options. To change a numeric value simply enter the new number. To change a toggled value press **LEFT**. The final option (POS ID) is an alpha-numeric value (use the keypad to enter numbers or text).
6. Select `save`.
7. Select `YES` to confirm.
8. Close your session.

### REPORT HEADERS & FOOTERS

Six header lines print at the top of all reports. You may edit these lines of text as follows:

1. Log in.
2. Choose `General Settings` then select `select`.
3. Choose `Headers` then select `select` (or choose `Footers` then select `select`).
4. Select `update` to enable editing of values. To edit use the keypad to enter numbers or text.
5. Press **DOWN** to move through each header line.
6. Select `save`.
7. Select `YES` to confirm.
8. Close your session.

### TYPES OF REPORTS

**Operator Report:** You may print either a summary or a detailed operator report for one or all operators. All of the information in the summary section is also included in the detail version. When an operator report is run that operator is automatically logged out of Insta Drop or Extended Drop. Financial information on an Operator Report includes all drop totals broken down by location and currency.

**Daily Close “Grand Z” or “End Day” Report:** This report is commonly called the End Day Report or Grand Z Report. This report may be run manually or may be configured to print automatically at a predetermined time each day. An Operator Report for each operator and a cash report will always be printed with this report automatically. Partial Day reports contain the same kind of information as the End Day Report except that they break down drop information before and after any cash removals during the business day. The final End Day report provides total system income data. Totals will be segregated by currency if more than one currency is configured in your system.

**Cash Report:** The Cash Report provides a breakdown of all money currently in the safe. You may choose whether to break down the subtotals by cash location or safe door. A bill count by denomination with monetary total is provided for each validator. The report ends with a grand total of all safe cashes (divided by currency, if applicable).

**User Report:** This report lists all enrolled users and their permissions. When printing this report you may select a summary or detailed version. You may also choose all users, only active users, or only inactive users.

**Audit Report:** The Audit Report is an exhaustive report of all system events. Note that financial data (drops, end day reports, deposit reports) are stored in their own audit histories separate from the system audit. Each event listed will include its transaction number, user number, date, time, user name and profile, then specific information about the event.

**Grand X Report:** This report is substantially the same as a Grand Z with regard to financial content, however it does not zero and reset the business day. Instead, it only reports the income of the current business day up to the point when it is run.

**Reference Report:** This report is similar to an Operator Report except that it is broken down by reference rather than user.

**System Information Report:** The System Information Report is an exhaustive report listing all configurable parameters in the system and their current settings. This report is normally only used by service personnel or at the request of the factory when troubleshooting.

**Supervision Configuration Report:** This is a highly specialized report normally used by service personnel for test purposes to check past remote connection history and present communication timing.

**Reprint Reports:** You may reprint previous Operator, End Day, and Cash Reports for any date in memory. In most cases you will have the same options as when you printed the original report. You may reprint only the most recent report or reprint each instance of the report for a range of dates.

## REPORT ELEMENTS

The following is a list of items that commonly appear on reports along with brief descriptions. Most reports contain several of these items and they appear in whatever order is most logical for the report at hand. These items are listed alphabetically for ease of reference:

Account #: Bank account number for deposits.

Date-Time: When listed near the top of a report this usually refers to the date and time the report is run. Following a reference to a Grand Z (End Day), it may refer to when the last Grand Z was run.

Device: List of devices being reported.

Enrolled: This is the date and time when the user was enrolled.

Event Cat: List of events being reported.

Footers: Three lines of text may be added at the end of all reports and receipts. These three lines function exactly like headers allowing you three additional lines for extra information.

From Date (listed immediately after "Last Grand Z"): This is the date and time of the start of the current business day (when the most recent End Day was run).

From Date (Audit Report): Start of audit period.

From Drop: All drops are numbered. This is the first drop number for this user on this business day.

Grand Z #: This is the ID number of this Grand Z (End Day) report.

Headers: Six lines of text may be at the top of all reports and receipts immediately below the logo. This is an ideal location to enter your business name, address, phone, and store number.

Key: Key code (not used).

Last Grand Z: Each End Day (Grand Z) Report is numbered. This is the number of the most recent Grand Z.

Last Login: Time of this user's most recent login.

Level: The user's profile title.

Logo: The FireKing Security Group logo prints at the very top of all reports and receipts.

Oper #: See "User #".

Oper Name: See "User Name".

Permissions: A complete list of specific permissions assigned to the user's profile is listed.

Personal ID: This is the number the user enters to identify themselves when they log in.

POS: This is a text string for the name of the POS device associated with the safe.

Printed By: (Immediately after the footers) the ID, name and profile of the user is printed.

Reference: References are used for record keeping purposes to distinguish sources for drops, such as departments or register numbers, etc.

Report Title: Immediately after the header lines the title of the report is shown for easy reference.

Status: User is active, inactive or deleted.

System ID: This is a text string for the name of the system.

Time: The time and date when the report was run.

To Date (Audit Report): End of audit period.

To Drop: This is the last drop number for this user on this business day.

Trans #: This is the transaction number in the audit history for the current event (the running of this report).

User: List of users reported on the Audit Report.

User #: Every user is assigned a User Number in the system (not the user's Personal ID). This number is used by the software for internal control.

User Name: This is the name of the user. The user's profile title usually prints next to the user's name.

## MAINTENANCE

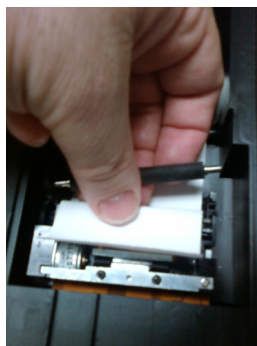
### CHANGING PRINTER PAPER

The display features an internally mounted thermal printer. When the paper is low a colored mark (generally red) will appear along the edges of each receipt. To change printer paper:

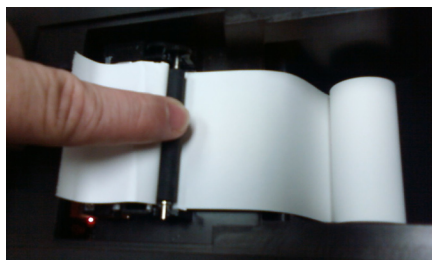
1. Remove the printer cover by pressing lightly and pushing toward the back.
2. Remove the roller from the printer so you can remove the paper roll.
3. Insert the new roll, checking to see that the paper always comes from underneath (only one side of the paper is usable).
4. Replace the roller in the printer. Make sure that sufficient paper is left to pass it through the slot of the printer cover.
5. Replace the printer cover (reverse the process described in step 1).
6. Press the paper advance button to verify that the new roll is installed correctly.



*Press and push to remove cover*



*Remove the roller*



*Roll from beneath, replace roller*

### REQUESTING FACTORY REPAIR

You may initiate a request for factory service by placing a phone call to NKL Technical Service (1.800.452.4655) or you may initiate the request through your control panel if your safe is properly configured and capable of network or GPRS (cellular phone) communication with the factory Edge-IP server. For more information refer to Sections 9 and 10. Initiate a repair request through your control panel as follows:

1. Log in.
2. Choose **Repair Order**.
3. Select **select**.
4. Use the **LEFT** button to choose the appropriate **Repair Type**.
5. Select **enter**.
6. Select **YES** to confirm.
7. Select **YES** to print a copy of the repair ticket.
8. Close your session.

### SILENCING THE BUZZER

In the event of an alarm condition that cannot be cleared (door locked open, sensor failure, etc.) use this procedure to silence the alarm:

1. Log in.
2. Choose **System**.
3. Select **select**.
4. Choose **Turn off buzzer**.
5. Select **select**.
6. Select **YES** to confirm.
7. Close your session.

### VALIDATOR CARE

At least once per month you should use validator cleaning cards. Enable the validator to make a drop (or simply validate a note) and insert the cleaning card. Do this three times. Use a fresh cleaning card for each validator. Certain validator types, such as the JCM "BNF bulk feed validator, may actually be removed from the safe without opening the safe door. If you have such a validator you may remove the validator head in order to clear bill jams. Always use extreme care when handling bill validators. Your organization may also have a maintenance agreement which provides for periodic preventative maintenance. Contact your area/district manager or call NKL Technical Service for more information.

## TROUBLESHOOTING

### MESSAGES

- **Message Invalid PIN or User:** The PIN entered does not match the user number or the user number is not enrolled. Reenter the PIN. If the PIN is lost, use the Edit Users procedure to set a temporary PIN.
- **Message Delay In Effect:** A delay is still counting down. Wait until the delay has expired, then try again.
- **Message Timelocked:** The door you are attempting to access is unavailable due to timelock. Wait until the door is out of timelock or use Armored Car override.
- **Message Violation Close Door:** 1) The door has been left open until the alarm time is reached. A constant audible tone alerts you to close the door. 2) The door is sensed open, but was not opened by procedure. 3) Door sensor failure (alarming with door shut). In the first or second case simply close the door. In the third case contact NKL Technical Service immediately.
- **Message Validator Full:** The validator mechanism senses that its cassette is full. Make a bank deposit (empty the bill cassette). *This may require your armored car service.*

### PROBLEMS

- **Door Will Not Unlock (No Error Message):** Possible internal cable problem, possible internal lock failure, possible boltwork jam or failure. Contact NKL Technical Service immediately.
- **Door Will Not Lock:** Something inside the safe is blocking the door or there is a problem with the mechanical boltwork. Check for and remove anything preventing the door from closing. If there is any sort of mechanical failure contact NKL Technical Service immediately.
- **Door Locked Open:** Perform the appropriate door opening steps of Section 2.8 to unlock the door, then close and lock the door normally.
- **Bill Jam (with or without error message):** The cassette is full, the validator is dirty or blocked by debris, or the validator has failed. Refer to Sections 5.4 or 5.5 (or supplemental material for other validator styles) for validator cleaning and jam clearing instructions. Empty the validator cassettes if full. In the event of validator failure contact NKL Technical Service immediately.
- **Receipt Indicates Unknown Denom:** A bill was accepted, but the validator was unable to determine its denomination. The likely cause is power interruption during a drop. Contact your manager for policy.
- **No Display:** The control panel is switched off or disconnected from the safe; loss of power to the safe; or component failure. Switch the control panel on, check the cable run from the control panel to the safe and the power supply to the safe; verify electrical power is available at the AC receptacle. If the problem cannot be found contact NKL Technical Service immediately.

## WARRANTY & SERVICE INFORMATION

### NKL WARRANTY INFO

NKL Safes have a one year or 90 day limited warranty depending on the specific model. Safes with one or more bill validators carry a 90 day base warranty. This would include any NKL safe model with a bill validator.

A Scheduled Maintenance Plan is available for most NKL safes at different levels to meet the diverse needs of each of our customers. Much like a copy machine, a cash handling safe has moving parts and is subject to wear and tear. Validators in particular are subject to environmental dirt, dust, lint and stray fibers from bills that can clog your validator over time. We recommend a scheduled maintenance plan to minimize bill jams and maximize business uptime.

**For complete warranty and scheduled maintenance plan information, terms, conditions, and the rest of the legalese please refer to our web site:**

**[www.fireking.com/safewarranty](http://www.fireking.com/safewarranty)**

### SERVICE (UNITED STATES)

To obtain warranty service, contact NKL Technical Support. Unauthorized service will void the warranty.

Maintenance agreements vary by customer. Please check with your corporate management or contact NKL Technical Service to determine which terms apply to your organization. For a copy of the current NKL warranty with complete details and terms visit our web site: [www.fireking.com/safewarranty](http://www.fireking.com/safewarranty).

NKL will service your product in or out of warranty. Obtain service (inside the United States) by contacting the NKL Technical Service:

NKL Cash Handling  
a member of FireKing<sup>®</sup> Security Group  
101 Security Parkway  
New Albany, IN 47150  
Ph 800.452.4655 / 812.948.8400  
[technicalsupport@fireking.com](mailto:technicalsupport@fireking.com)

Normal business hours are 8 am to 5 pm E.T., however the NKL Technical Service is available 24 hours a day, 7 days a week. Between 8 pm and 8 am (E.T.) and after 4 pm on Sundays or holidays you may leave a message and a technician will be paged to return your call, typically within minutes.

NKL reserves the right to deny warranty service in cases of abuse or misuse.

### SERVICE (INTERNATIONAL)

To obtain warranty service, contact your dealer or distributor. Unauthorized service will void the warranty. Special conditions may apply to customers outside the United States.

Outside the United States, NKL provides warranty parts at no charge (not including tariffs).

NKL and its international distributors reserve the right to deny warranty service in cases of abuse or misuse.



a member of FireKing<sup>®</sup> Security Group  
101 Security Parkway  
New Albany IN 47150  
Phone 800-452.4655 / 812-948-8400  
[www.fireking.com](http://www.fireking.com)